ATILS

Comments by Joshua Walker, Task Force Member, AI Subcommittee

Recommendation not yet voted on by the Task Force: If an entity is permitted to practice law using technology, then that entity should be required to provide adequate privacy protections similar to the protection afforded by the attorney-client privilege and a lawyer's ethical duty of confidentiality.

This note covers privacy, privilege, and confidentiality in a legal technological medium. The above duties exist for good reasons. We will not recount them here as they are best retold in the relevant legislative histories and case law. But, for example: We do not want a law firm "stealing" or "leaking" information from one client to benefit another, or to secretly benefit herself. Nor do we want attorneys leaving litigation files in cafes. The duty requires diligence, and enjoins against informational abuse. The privilege, in turn, helps encourage broad and open communication between the legal function and the client, a meritorious goal in itself.

We impose such duties on human lawyers. Why should we impose a lesser burden on technological platforms carrying out identical functions? In many ways, it is easier to control information in a unitary technological platform than in a law firm. Where well designed, the former may better facilitate singular tracking and control.

There are both political and functional reasons to impose analogous confidentiality burdens on platforms. First, a task force recommendation (or the absence of recommendation) that treats legal data like any other type of consumer data is unlikely to be further promulgated. The state, and the country (indeed much of the world) is in the middle of a backlash against commercial misuse of even nonmaterial consumer data. How much more so will the public and the legislature prioritize vital legal information? Second, the absence of suitable confidentiality controls on technologies is likely to be deleterious to the profession, where traditional lawyers will be informationally disadvantaged to big platforms with limited or no real privacy constraints. Third, and more importantly, it is likely to harm clients, for the exact same reasons that justified the privilege and the duty of confidentiality itself. Lastly, we want to encourage frank disclosure of critical legal data to the relevant technological medium, for the same reason we want to encourage frank disclosure to attorneys in person. The absence of some form of privilege protection is likely to chill the functionality of advanced legal systems.

We cannot assume regulatory identity. We will have to *transcribe*, not directly proscribe, these duties upon new means of carrying out the legal function. In other words, there may be instances where we allow a single technological platform to process information from many clients, including—potentially—clients adverse to one another. However, such a platform must prove that the fundamental purposes of confidentiality and privacy are being satisfied. For example, it cannot leverage the data of one client to help another client that pays more. With limited exceptions, it should not sell specific client data to third parties. Legal clients of such

platforms must have rights to their data comparable to those consumers retain over their medical data, even as we make the processing and management of legal rights more efficient, and more scalable and affordable to more people.